F-Secure Mobile Security with Parental control

Android

目次

第 1 章：インストール.....5
インストール.....6
認証.....6
F-Secure Mobile Securityを設定する.....7
F-Secure Mobile SecurityをAndroidデバイスからアンインストールする.....7

第 2 章：データの保護をする.....9
リモートアンチセフトを有効にする.....10
リモートロック.....10
リモート削除.....10
リモートロケート.....11
SMS警告.....11
アンチセフトのアラームを使用する.....11
位置情報を共有する.....12

第 3 章：ブラウザ保護.....13
ブラウザ保護を使用する.....14
デフォルトのブラウザを変更する.....14
インターネットを安全に利用する.....14
ブラウザ保護を有効にする.....14

第 4 章：ウイルスをスキャンする.....17
マニュアル スキャン.....18
感染したファイルの処理.....18
ウイルス保護の設定を変更にする.....18

第 5 章：お子様/未成年に安全なインターネット環境を設定する.....21
ユーザプロフィール.....22
コンテンツタイプ.....22
ユーザプロフィールを指定する.....23

第 6 章：F-Secure Mobile Securityを更新する.....25
更新モードを選択する.....26

手動更新.....26

第 **7** 章：ライセンス.....**27**

コンピュータを使用してライセンスを購入する.....28

第
1
章

インストール

トピック：

- *インストール*
- *認証*
- *F-Secure Mobile Securityを設定する*
- *F-Secure Mobile SecurityをAndroidデバイスからアンインストールする*

ここでは、F-Secure Mobile Securityをモバイルのデバイスにインストールするための方法を説明します。

製品をデバイスにインストールする方法を選択します。

- インストーラをコンピュータにダウンロードして、デバイスに転送する
- インストーラをデバイスに直接ダウンロードする

F-Secure Mobile Securityのインストール後、ライセンスを認証してください。ライセンスを認証したら、デバイスが保護されます。

インストール

Mobile Securityをモバイルデバイスにインストールする方法について説明します。

Mobile Securityを旧バージョンからアップグレードする場合、旧バージョンをアンインストールする必要はありません。アップグレード後、Mobile Securityの設定が正しく継承されていることを確認してください。

Mobile Securityをインストールするには

1. 設定 > アプリケーション の順に選択して、[不明なソース] が有効になっていることを確認します。

   この設定が有効な場合、Android Market以外のアプリケーションをインストールできるようになります。
2. インストーラをコンピュータにダウンロードして、デバイスに転送します。または、インストーラをデバイスに直接ダウンロードします。

   詳細については、デバイスの取扱説明書を参照してください。
3. デバイスでインストーラを実行します。

   メモリカードからインストーラを実行する場合、サードパーティのファイルマネージャが必要になります。

   Mobile Securityがデバイスにインストールされます。
4. インストール後、[開く] を選択して、アプリケーションを認証します。

Mobile Securityを認証しない限り、デバイスは保護されません。

認証

ライセンスを認証すると、デバイスに対する保護が有効になります。

ライセンスを認証するには

1. F-Secure Mobile Securityを起動します。
   ライセンスの使用許諾契約書が表示されます。
2. 内容を確認し、同意する場合、[**OK**] を選択します。
   ライセンスの認証手続きが始まります。
3. 認証タイプを選択します。

   Mobile Securityは「無料評価」モードまたはライセンスキーコードで認証できます。ライセンスのタイプにより、Anti-theftまたはMobile Securityの機能を利用できます。

   - [無料評価] を選択すると、ライセンスキーコードを入力する必要はありません。Mobile Securityが期限付きの評価ライセンスで動作します。
   - ライセンスキーコードをお持ちの場合、[ライセンスキーコード] を選択してキーコードを入力します。
4. [認証] を選択します。

   👉 **注:** 認証中にMobile Securityはエフセキュアの更新サービスに接続します。

認証後、製品の機能を設定できるウィザードが開きます。

Android 2.2以降のOSを利用している場合、アンチセフトを利用するためにデバイス管理者を有効にする必要があります。

F-Secure Mobile Securityを設定する

F-Secure Mobile Securityを使用する前に製品の設定を行う必要があります。

次の方法でアンチセフトとペアレンタルコントロールを有効にできます。

1. セキュリティコードを作成します。
   アンチセフトのリモート機能とペアレンタルコントロールを利用するにはセキュリティコードが必要となります。
2. デバイスの管理を行うための認証を行います。デバイス管理者を認証するために [認証] を選択します。
3. デバイスのスクリーンロックを設定していない場合、スクリーンロックを設定します。
   詳細については、デバイスの取扱説明書を参照してください。
4. 信頼済みの電話番号を入力します。
   デバイスのSIMカードが変更されたときに信頼済みの電話番号に通知が送信されます。
5. ペアレンタルコントロールを設定するためにデバイスを利用するユーザの年齢層を選択します。

アンチセフトとペアレンタルコントロールを設定したら本製品が有効になります。

F-Secure Mobile SecurityをAndroidデバイスからアンインストールする

デバイスからF-Secure Mobile Securityをアンインストールする方法について説明します。

F-Secure Mobile Securityをアンインストールするには

1. メインビューで [設定] を選択します。
2. 「 設定」メニューから [一般] を選択します。
3. [アンインストール] を選択します。
   アンチセフトのセキュリティコードを作成した場合、アンインストールを行うためにセキュリティコードを入力する必要があります。

F-Secure Mobile Securityがデバイスから削除されます。

👉 注: 「デバイス管理者」の一覧で本製品が無効になります。アンインストールをキャンセルすると、製品をもう一度認証する必要があります。

第
2
章

データの保護をする

トピック：

- *リモートアンチセフトを有効にする*
- *SMS警告*
- *アンチセフトのアラームを使用する*
- *位置情報を共有する*

アンチセフトを使用すると、デバイスを紛失した場合でもデバイスの本体とデータを保護することができます。

デバイスを紛失しても、デバイスにSMSを送ることでデバイスをロックすることが可能です。

- 一度デバイスをロックすると、アンロックパターンを利用しない限り、デバイスのロックを解除することはできません。

  👉 注: 「リモートロック」を使用するには、デバイスのアンロックパターンを有効にする必要があります。

「リモート削除」は、デバイスのデータをリモートから削除する機能です。

- デバイスにリモート削除を指定するSMSを送ると、デバイスのデータ (SD カード、SMS/MMSメッセージ、連絡先、カレンダーの各データ) が削除されます。リモート削除を行う場合、セキュリティのためにGoogleアカウントをパスワードを変更することも推奨します。
- Android 2.2以降のOSを利用している場合、リモート削除のSMSをデバイスに送るときにデバイスの全設定が初期化されます。

リモートアンチセフトを有効にする

リモートアンチセフトを有効にすると、デバイスにSMSを送ることでデバイスのロックまたはデータの削除を行うことが可能になります。

リモートアンチセフト設定するには

1. メインビューで [アンチセフト] を選択します。
2. 「アンチセフト」メニューから [設定] を選択します。
3. デバイスの位置をリモートから検出できるようにするには、[ロケータを有効にする] を選択します。
   ロケータを使用するには、デバイスのGPS機能が有効であることを確認してください。通常、この機能はデフォルトで有効になっています。詳細については、デバイスの取扱説明書やヘルプを参照してください。
4. [リモートアンチセフト] を選択します。

リモートアンチセフトが有効になります。

リモートロック

「リモートロック」は、デバイスをリモートからロックして、第三者がデバイスを使用することを阻止します。

デバイスをリモートからロックするには

1. 次の内容を持ったSMSをデバイスに送ることでデバイスをロックできます。`#LOCK#<セキュリティコード>`
   (例: `#LOCK#12345678`)
2. デバイスをロックすると、ロックSMSを送信した電話へ返信メッセージが送られます。リモートロケールを有効にした場合、デバイスの位置情報が返信メッセージに含まれます。

一度デバイスをロックすると、設定したスクリーンロックを利用しない限り、デバイスのロックを解除することはできません。

リモート削除

「リモート削除」は、デバイスのデータをリモートから削除して、第三者がデバイスのデータを使用することを阻止します。

リモートからデバイスのデータを削除するには

1. 次の内容を持ったSMSをデバイスに送ることでデバイスのデータを削除できます。`#WIPE#<セキュリティコード>`
   (例: `#WIPE#12345678`)
2. リモート削除を行うと、SMSを送信した電話へ返信メッセージが送られます。

リモート削除を行うと、SD カード、SMS/MMSメッセージ、連絡先、カレンダーの各データが削除されます。Android 2.2以降のOSを利用している場合、リモート削除のSMSをデバイスに送るときにデバイスの全設定が初期化されます。

リモートロケート

デバイスを見失った場合、デバイスにSMSを送ることでデバイスの位置を検索することが可能です。

👉 注: デバイスの位置情報を検索するには、デバイスのGPS機能が有効になっている必要があります。

デバイスの位置を検索するには

次の内容を持ったSMSをデバイスに送ることでデバイスの位置を検索できます。#LOCATE#<セキュリティコード>
(例: #LOCATE#12345678)

しばらくしてからデバイスの位置を知らせるSMSが届きます。

👉 ヒント: 本製品をデバイスにはじめて設定するときには、リモートロケート機能の動作を確認するためにロケート用のSMSを検証用に送ることを推奨します。

👉 注: アンチセフトはSMSを通じてデバイスの位置データを送りますが、そのデータを保存することはありません。

SMS警告

アンチセフトは、デバイスのSIMカードが変更された場合にSMSを別のデバイスに送る「SMS警告」機能を搭載しています。

SMS警告を有効にするには

1. メインビューで [アンチセフト] を選択します。
2. 「アンチセフト」メニューから [設定] を選択します。
3. [信頼済みの番号] を選択します。
   「信頼済みの番号」を設定する画面が開きます。
4. SIMカード変更時に送るSMSの送信先 (電話番号) を指定します。

SMS警告が有効になります。

アンチセフトのアラームを使用する

デバイスの紛失や盗難時にアラーム (警告音) を鳴らすことができます。

アラームを設定するには

1. To play an alarm, send the following SMS message to your device: #ALARM#<security code>#<repeat count>

   👉 注: 再生回数でアラームを鳴らす回数を指定できます (指定しなくてもアラームは鳴ります)。

   (例: #ALARM#abcd1234)
2. SMSを受信すると、デバイスがロックされ、アラームが鳴ります。SMSを送信した電話へ返信メッセージが送られます。

設定したスクリーンロックを利用することでアラームを無効にできます。

👉 ヒント: You can turn off the alarm remotely by sending the following SMS message to your device: `#ALARM#<security code>#0`

位置情報を共有する

友達や家族に自分の位置情報を知らせるメッセージを送ることができます。

位置情報を共有するには、デバイスのGPS機能を有効にする必要があります。

位置情報を共有するには

1. メインビューで [アンチセフト] を選択します。
2. 「アンチセフト」メニューから [位置情報の共有] を選択します。
   本製品がGPS機能を使用して位置情報を取得し、メッセージアプリケーションを開きます。
3. メッセージアプリケーションで位置情報を知らせる宛先を指定して、[送信] を選択します。
   メッセージに位置情報と現在地を示すGoogleマップのリンクが含まれます。

第
3
章

ブラウザ保護

トピック：

- *ブラウザ保護を使用する*
- *インターネットを安全に利用する*

ここでは、ブラウザ保護の機能について説明します。

ブラウザ保護は個人情報 (クレジットカード情報、ユーザアカウント情報、パスワードなど) を盗むWebサイトからユーザを保護します。

ブラウザ保護を使用する

ブラウザ保護を活用するにはF-Secure Browserを使用する必要があります。他のブラウザではブラウザ保護は機能しません。

次の方法でブラウザ保護をブラウザで利用できます。

ブラウザを起動するには

- 本製品の専用ブラウザ(セーフブラウザ)を開きます。メインビューで、[ブラウザ保護] のオプションから [セーフ ブラウザ] を選択します。
- Android のランチャーから [**F-Secure Browser**] を開きます。

デフォルトのブラウザを変更する

デバイスのデフォルトブラウザを変更する方法について説明します。

F-Secure Browserはデフォルトのブラウザとして自動的に設定されません。次の方法でF-Secure Browserをデフォルトのブラウザに設定できます。

1. **[**設定**]** > **[**アプリケーション**]** > **[**アプリケーションの管理**]** の順に押します。
2. [ブラウザ] を選択します。
3. [デフォルトでの起動] で [設定を消去] を選択します。
4. [**F-Secure Browser**] をデフォルトのブラウザに設定します。

インターネットを安全に利用する

ブラウザ保護を使用すると、危険性のあるWebサイトにアクセスすることを防ぐことができます。

Webページにアクセスする際にWebページの安全性が自動的に確認されます。アクセスしようとしているWebページが「不審」または「危険」と評価されている場合、Webページのアクセスがブロックされます。Webページの評価は、エフセキュアのマルウェア分析やパートナーからの調査などによって基づいています。

ブラウザ保護を有効にする

利用しているプロバイダに応じて、ブラウザ保護を有効にするか指定できます。

ブラウザ保護を設定するには

1. メインビューで [設定] を選択します。
2. [ブラウザ保護] を選択します。
3. [ブラウザ保護] を有効にします。
4. ブラウザ保護のプロバイダ設定を指定します。
   - 全プロバイダ - ブラウザ保護を常に有効にします。旅行や海外にてプロバイダが変わった場合でもブラウザ保護が有効になります。
   - マイプロバイダ - 指定のプロバイダネットワークに接続している場合にのみブラウザ保護が有効になります。

ブラウザ保護を有効にすると、危険なWebサイトがブロックされるようになります。[戻る] を選択すると、前の画面に戻れます。

ブロックしたWebページで表示される [**Web**ページにアクセスする] リンクをクリックすると、ブロックしたページにアクセスすることが可能です。

第
4
章

ウイルスをスキャンする

トピック：

- *マニュアル スキャン*
- *感染したファイルの処理*
- *ウイルス保護の設定を変更にする*

F-Secure Mobile Securityはデバイスに対してウイルスと悪質なコンテンツのスキャンを行います。

F-Secure Mobile Securityは、インストール済みのプログラムおよびデバイスに装着されているメモリーカードに対してウイルス、スパイウェア、リスクウェアのスキャンを行います。

👉 注: F-Secure Mobile Securityがデバイスをスキャンするよう警告を表示したときにはスキャンを実行することを推奨します。

マニュアル スキャン

必要に応じて、手動でウイルスのスキャンを実行することができます。

手動でスキャンを実行するには

1. メインビューで [ウイルス保護] を選択します。
2. [今すぐスキャン] を選択します。
   ウイルススキャンが開始します。
3. スキャンが完了したら、次の情報が表示されます。
   - 感染 - 検出された感染の数を示します。
   - 未スキャン - スキャン中にスキャンされなかったファイルの数を示します。別のプログラムがファイルを使用している場合やファイルが破損または暗号化されている場合、ファイルはスキャンされません。
   - スキャン済み - スキャンされたファイルの数を示します。
4. [戻る] を選択してスキャンを終了します。

感染したファイルの処理

特定のファイルに感染が検出された場合、感染したファイルをデバイスから削除することができます。

感染したファイルを処理するには

1. メインビューで [ウイルス保護] を選択します。
2. [感染したファイル] を選択します。
   「」画面で感染したファイルの一覧が表示されます。
3. から処理するファイルを選択します。
4. 感染したファイルを選択すると、ファイルの詳細を確認できます。「感染の詳細」画面では、感染したファイルのパスと名前、および感染の原因となるウイルス名が表示されます。
5. [削除] または [アンインストール] を選択すると、感染したファイル/アプリケーションを取り除きます。

ウイルス、トロイの木馬、ワーム、その他のマルウェアに関する追加/詳細情報は、エフセキュアのWebサイト (*http://www.f-secure.com/virus-info/*) でご覧になれます。

ウイルス保護の設定を変更にする

ウイルスの保護レベルを変更することで、ウイルス スキャンを実行したいときを選択できます。

ウイルス保護の設定を変更にするには

1. メインビューで [設定] を選択します。
   設定画面が開きます。
2. [ウイルス保護] を選択します。
3. [インストールスキャン] - プログラムをインストールした後にスキャンします。

4. [メモリーカードスキャン] - メモリーカードをデバイス装着時にスキャンします。

第
5
章

お子様/未成年に安全なインターネット環境を設定する

トピック：

- *ユーザプロフィール*
- *ユーザプロフィールを指定する*

ペアレンタルコントロールはお子様/未成年がインターネット上の望ましくないコンテンツにアクセスすることを阻止します。

インターネットには数多くの面白いWebサイトがある反面、お子様や未成年に危険性があるのも事実です。お子様/未成年のユーザはモバイルデバイスを利用してインターネットにアクセスすることが一般的になっており、ほとんどの場合その行動は監視されていません。多くのWebサイトにはお子様や未成年に対して望ましくないコンテンツが含まれているため、お子様/未成年がそのようなコンテンツさらされてしまうことは簡単です。また、ウイルスなどの不正なファイルを誤ってダウンロードしたり、嫌がらせのメールを配信されたりすることも可能です。

ペアレンタルコントロールを利用することで、お子様/未成年のユーザが不正なコンテンツにアクセスすることを制限できます。

ユーザプロフィール

「ユーザプロフィール」を利用して、ティーンエイジャとチャイルドプロフィールのユーザがアクセスできるWebサイトのカテゴリを指定することができます。

ペアレンタルコントロールはユーザがアクセスしようとするWebページを分析し、コンテンツに基づいて望ましくないWebページをブロックします。

ペアレンタルコントロールには異なるコンテンツを制限するプリセットのプロフィールが3つ搭載されています。「ティーンエイジャ」プロフィールは一部のコンテンツに対するアクセスを制限し、「チャイルド」プロフィールにはより厳しい制限が適用されます。「成人」プロフィールのユーザはインターネットを制限なくアクセスできます。

ユーザプロフィールはインストール時に、またはペアレンタルコントロールの設定ページで後から設定することができます。

コンテンツタイプ

ペアレンタルコントロールを使用して、コンテンツ別にWebサイトのアクセスをブロックすることができます。

- アダルト

  性的な表現や性描写を含む成人向けのコンテンツを示します。アダルトショップやヌードなどの性的コンテンツ。
- チャット

  Webベースのチャットプログラムやインスタントメッセージ用ソフト、チャットサイトなど。
- Webメール

  メールアカウントを作成できるサイトやブラウザを通じてメールを送受信できるサイトなど。
- 武器

  武器の写真や説明、爆弾の作り方を含むサイトなど。
- ギャンブル

  オンラインカジノ、ギャンブル関連のWebサイトなど。
- 麻薬

  薬物使用を促すサイト。麻薬の栽培や売買に関する情報を含むサイトなど。
- 出会い系

  出会い系やメールオーダーブライドのサイトなど。
- ソーシャルネットワーク

  プライベートやビジネスの交流に関する社会的ネットワークを提供するサイトなど。
- 掲示板

  コメントを表示/投稿できるオンライングループや掲示板を作成できるプログラムなど。
- ブログ

  オンラインの日記や個人Webページ、ブログ、ポッドキャストなど。
- ショッピングとオークション

Web上で商品を直接注文できるサイトや価格比較、インターネットのオークションサイトなど。

- カルト

  宗教、その他のイデオロギーに反対する熱狂的なグループを支援するサイトなど。

- お酒とタバコ

  お酒やタバコに関する製品の情報を提供、促進、支援するサイトなど。

- 憎悪表現と暴力

  特定の宗教、人種、民族、性別、年齢層、障害者、性的指向に対する差別を示すサイト、または暴力、動物虐待、機関への破壊行為に関する写真や説明を含むサイトなど。

- 違法ダウンロード

  プログラムの違法/不審なアクセスを提供するサイト、またはネットワークやシステムに問題を発生させるプログラムを開発および配布するサイトなど。

- アノニマイザー

  インターネットの行動を追跡できないようにするサイトやフィルタを回避する情報を提供するサイトなど。

- 不明

  コンテンツが認識されないサイトは、「不明」のカテゴリとして指定されます。

ユーザプロフィールを指定する

ユーザプロフィールを利用して、デバイスのユーザを指定することができます。ペアレンタルコントロールはプロフィールに基づいてWebコンテンツを制限します。

ユーザプロフィールを変更するには

1. メインビューで [設定] を選択します。
2. [ペアレンタルコントロール] を選択します。
3. [ペアレンタルコントロール] を有効にします。
4. [年齢層] でユーザプロフィールを指定します。
   年齢層によって、ユーザがアクセスできるカテゴリが異なります。
5. [カテゴリ] を選択すると、カテゴリを表示/編集できます。
6. 許可するカテゴリを指定します。

年齢層/ユーザプロフィールを変更すると、Webページのアクセスは、ペアレンタルコントロールが許可したページに限定されます。

第
6
章

F-Secure Mobile Securityを更新する

トピック：

- *更新モードを選択する*
- *手動更新*

F-Secure Mobile Securityの「自動更新」機能は、ウイルスの定義ファイルやプログラム本体を自動的に更新する機能です。

F-Secure Mobile Securityを認証した時点で自動更新が有効になります。自動更新はインターネットに接続している際に更新を確認し、更新がある場合には更新をダウンロードします。

👉 注: F-Secure Mobile Securityの自動更新機能は有効なライセンスを必要とします。

更新モードを選択する

F-Secure Mobile Securityをインストールしたら自動更新が有効になります。自動更新またはリアルタイムスキャンを無効にした場合、更新を手動で行う必要があります。

更新モードを選択するには

自動更新のモードを選択します。

- 有効 - 更新を定期的にダウンロードして、ウイルス定義ファイルを最新の状態にします。(推奨)
- ホームネットワーク内 - デバイスがホームネットワークに接続している場合、更新を自動的にダウンロードします。
- 無効 - ウイルス定義ファイルを自動的に更新しないようにします。自動更新を無効にすることは推奨しません。

手動更新

Mobile Securityを手動で更新することもできます。

更新を手動で確認するには

1. メインメニューで [更新] を選択します。
   更新を確認するにはインターネットの接続が必要です。
2. [はい] を選択します。
   新しい更新が利用できる場合、ダウンロードの確認が表示されます。
3. [はい] を選択して、更新をダウンロードします。
4. ダウンロードが完了したら、インストール] を選択します。

第
7
章

ライセンス

トピック：

- *コンピュータを使用してライセンスを購入する*

Mobile Security の保護を継続的に使用するには有効なライセンスが必要です。この理由で、ライセンスが切れる前に追加のサービス期間を購入することを推奨します。

F-Secure Mobile Security のライセンスはいくつかの方法で購入できます。

- F-Secure eStore
- お近くの販売店
- プロバイダが継続的なライセンスを提供

F-Secure Mobile Securityの無料評価モードまたはF-Secure Anti-Theftを使用している場合、「購入」メニューからF-Secure Mobile Securityにアップグレードすることができます。

コンピュータを使用してライセンスを購入する

コンピュータを使用してMobile Securityのライセンスを購入することができます。

コンピュータを使用してライセンスを購入するには

1. Web ブラウザから *http://www.f-secure.com/estore/avmobile.shtml* にアクセスします。
2. [ライセンスキーコード] フィールドにライセンスキーコードを入力します。
   クレジットカードでライセンスを購入できます。
3. 画面上に指示に従って取引を完了します。